ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

A Framework to Achieve Data Security and Privacy in Cloud Computing

Dipti Sen, Prof. Pradeep Tripathi

M. Tech Research Scholar, Department of Computer Science & Engineering, Vindhya Institute of Technology and Science - [VITS, SATNA], India

Professor & Head of the Department, Department of Computer Science & Engineering, Vindhya Institute of Technology and Science - [VITS, SATNA], India

ABSTRACT: Cloud Computing is the most promising technology which increases rapidly as increasing years. In Cloud Computing environment, the data of the user is stored in the server and security of the data be blame to service providers of the company. The service provider taken care of the security for the data of the customers. In the cloud computing system, the problem is that the service providers treating all the data in the same manner means they provide common security to all the data for the particular user without considering that whether that required that security or not. So as a solution for this problem, we proposed the concept of data classification. In our proposed work, we categorize the data into categories based on the secrecy of the data and particular category of the data is secured with respective level of security. By using this concept we can reduce the overhead and increased the processing time. Also it can increase the performance of the cloud environment. The proposed work is using different encryption algorithm for the security of the data. Using our work, data which required high security they get high, and which want the low security they get low. As compared to the existing solutions, which encrypt all the data with single encryption algorithm, this work is more secured and efficient.

KEYWORDS: Cloud Computing, Data Security, Data Classification, File Splitting Security.

I. INTRODUCTION

Now a day's Cloud Computing Technology is the most promising Technology comes in the real world. Users are more aware of the advantages of the Cloud Computing and they start using it. Cloud Computing is the next generation system which provides an easy and customizable way of managing data in the Internet. It provides the user various services of accessing and work with the application of Cloud. Users can upload their data in the Cloud Storage and can access through anywhere through any devices like Laptop, Desktop, Mobile etc. Data is the necessary, essential and a valuable thing belongs to users. Data can be in any format like documents, videos, pictures etc. Whenever the discussion of data comes some of the properties of data emerges. Some of them are Accuracy, Completeness and Consistency etc.

Data in Cloud is mainly deals with 3 security issues Confidentiality, Integrity and Availability. Data Confidentiality means data should be confidential to others. Unauthorized or Unauthenticated users can't able to access or use the data. Data Integrity means content of the data should not be violated. It is said that we have to maintain data for achieving consistency and accuracy. When the user want to access the data the data should be available for them, this is called Availability. For achieving the availability of the data proper storage type, proper recovery and backup management has to be implemented.

Cloud Service Providers (CSPs) trying to offer their clients the same type of environment as the client get from the Internet Service Providers (ISPs). Like both offers the administrations, both are working in the Distributed Environment etc. Distributed Computing added some more advantages on Cloud Computing as it power up the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

Computing, provide the customer to access the system in their interest. The Distributed Computing Innovation faces some of the issues regarding security.

II.ISSUES IN CLOUD ENVIRONMENT

The three deployment models are private cloud, public cloud and hybrid cloud. The security issues of these deployment models are discussed below [6].

A. Security issues in a public cloud

In a public cloud model, the platform and infrastructure are shared among customers. The securities for these services are provided by the cloud service provider. A few of the key security issues in a public cloud include:

1) Since there is no control over the security mechanisms used by the cloud service provider, it is difficult to protect data in all its stages providing the basic requirements of confidentiality, integrity and authenticity.

2) Since most service providers use a multitenant architecture hence the possibility of data leakage between the tenants is very high.

3) If the Cloud service provider uses a Third Party vendor for providing the services, then there is added overhead of verifying the agreements and contingency plans between them.

4) There is also a possibility of an insider attack at the service provider side. As the cloud architecture grows the number of insiders grow. Proper laws should be enforced to protect data from malicious insiders.

B. Security issues in a private cloud

A private cloud model enables the customer to have local network and storage space. They provide the flexibility to the customer to implement any kind of required services. There are certain securities issues:

1) Due to virtualization, unauthenticated and unauthorized access to system is possible

2) Malware can be used to attack the host operating system.

3) Security policies must be designed to protect attacks from insiders.

The hybrid cloud model is a combination of both public and private cloud and hence the security issues discussed with respect to both are applicable in case of hybrid cloud model. Each of the three ways in which cloud services can be deployed has its own advantages and limitations. And from the security perspective, all the three have got certain areas that need to be addressed with a specific strategy to avoid them [6].

III. LITERATURE REVIEW

There are various work done in the field of Cloud Computing. Many methods and work have been proposed related to security in Cloud. Some are discussed below:-

Rizwana Shaikh, M. Sasikumar, This paper is the survey paper which surveyed the security issues in cloud computing. The author is this proposed the different security concerns, what are the security issues the Client and the Providers facing in the Cloud Computing. For some of the issues he also focuses on the solutions.[1]

Mr. Rupesh R Bobde, Amit Khaparde and Dr.M. M. Raghuwanshi proposed a scheme in which the original data get sliced into different slices. The data in each slice can be encrypted by using different cryptographic algorithms and encryption key before storing them in the Cloud. The objective of this technique is to store data in a proper secure and safe manner in order to avoid intrusions and data attacks meanwhile it will reduce the cost and time to store the encrypted data in the Cloud Storage.[3]

Lo'ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, Fahd Aldosari, In this paper the author find out the problem in Cloud Computing and the problem is treating all the data in same manner and providing same level of security. As a saluting for the above problem he proposed a framework which classify the data into three categories say Basic, Confidential and High Confidential and providing the different security techniques according the requirement like Basic get very less security, Confidential get moderate security and High Confidential get High security.[4]

Gurpreet Singh and Miss Supriya performed a detailed study of the popular Encryption Algorithms such as RSA, DES, 3DES and AES. In this paper, a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which might be suitable

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

for different applications and has its own pro's and con's. They found that AES algorithm is most efficient in terms of speed, time, and throughput and avalanche effect. [5]
Ritu Tripathi, Sanjay Agrawal performed a survey on symmetric and asymmetric cryptographic methods. This paper presents a performance evaluation of selected symmetric and asymmetric encryption algorithms such as DES, 3DES, AES, Blowfish, RSA and Diffie Hellmen The key length is higher at the Asymmetric encryption technique .The high key length makes to break the code complex in RSA. In the aspect of throughput, Throughput is increased so power consumption is decreased. Throughput is high in blowfish and blowfish is less power consumption algorithm hence speed is fast in the Symmetric key encryption is viewed as good. Finally, in the symmetric key encryption techniques the blowfish algorithm is specified as the better solution. In the Asymmetric encryption technique the RSA algorithm is more secure since it uses the factoring of high prime number for key generation. [6]

IV. PROBLEM STATEMENT

According to the literature review we have find out that in the entire Cloud Computing environment, there is a problem that all the organizations, using the single software for the encryption of the data. Single Software means they all treat whole data in a same manner. This is the drawback of using single software for the security without considering the sensitiveness or criticalness of the data. Now after the detection of the problem the solution for this is the classification of the data. Classify data into categories and according to that provide Security.

V.PROPOSED SYSTEM

In our proposed work we have categorize or classify the data into three categories: General Data, Secured Data and Highly Secured Data. In our work the classification done manually means the users themselves classify the data. The reason for making the classification manual is that every user knows there data better than others. He only knows that out of their data, which data is actually required more security or not. And the user also get freedom of selecting which data he wants to secured more or less.
General Data: In general data, all the data which the users want to be secured with less security reside in this. The data which comes in this category they get lower level security. For lower level security we are using AES 128 Encryption algorithm.
Secured Data: This is another category in which the data which required moderate security comes here. Moderate security means security which is higher than General data but lower than High Secured data. For Secured Data we are using the AES 256 bit encryption algorithm.
Highly Secured Data: This is category which provides the highest security to data. The data which reside in this category, all that data are secured with best security mechanism. Here in our proposed work, for high security we uses the concept of File Splitting where whole file is divided into 3 chunks and each chunks is secured with TDES, AES-128 and AES-256.
File splitting: In our proposed work we have used a concept called File Splitting. File Splitting is the technology or mechanism which divides the particular files into chunks. Here chunks are used for denoting the small parts of files. So the chunks are then stored in different location and when that file is required then all the chunks from their location fetched up and merged to form the original file. The main importance of the file splitting is to increase the execution time. The situation the file splitting is going to be a good option where execution time important factor as splitting file into chunks and execute each chunks may reduce the processing time.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

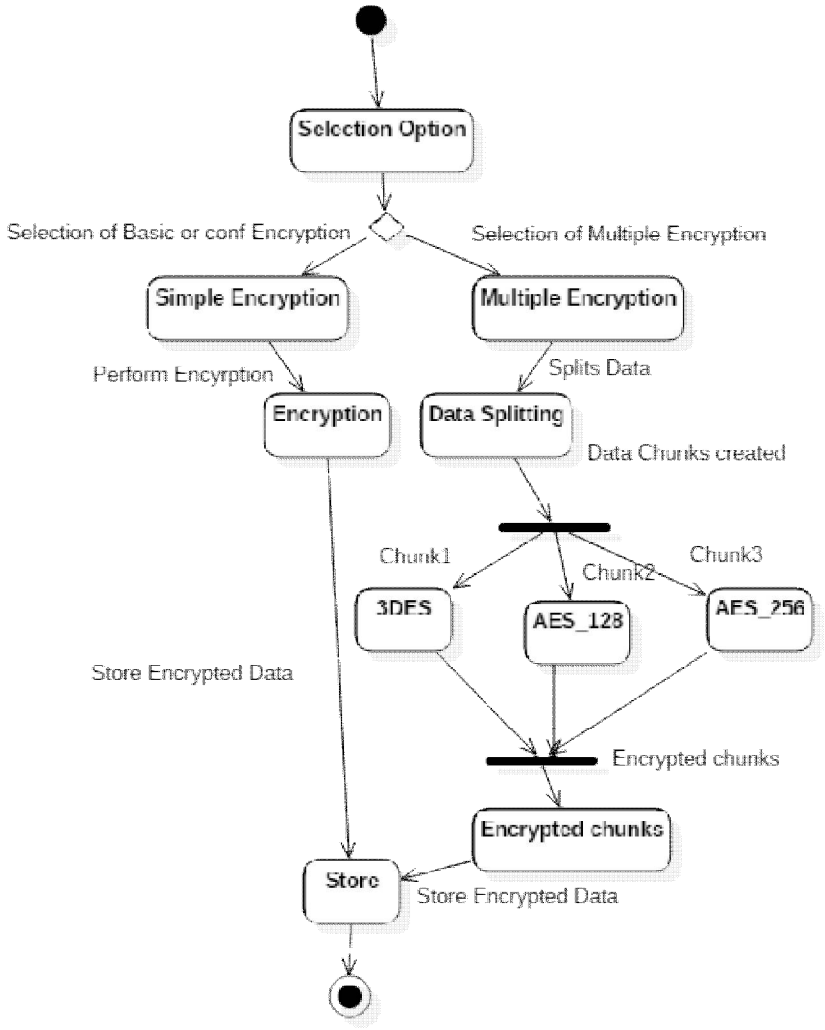


Fig 1: State chart diagram for Overall System

VI.RESULT AND COMPARISON

For the implementation of our proposed work, we have created a web environment same as the user get in cloud. The user has an interface containing upload file and show file then he have to choose either upload the file or view their previously uploaded file. When the user selects the "Upload File" option, he has moved to the browser page where he has to choose the file from their local storage. After chosen the file, he also has to choose the respective security which he wants for the uploaded data, and accordingly encryption security will be provided to the data of user.We find out the time taken by the different options chosen by the user either it is general, secured or highly secured and compared them and find out the given result. We have used AES128 for general, AES256 for secured and file splitting for highly secured category.

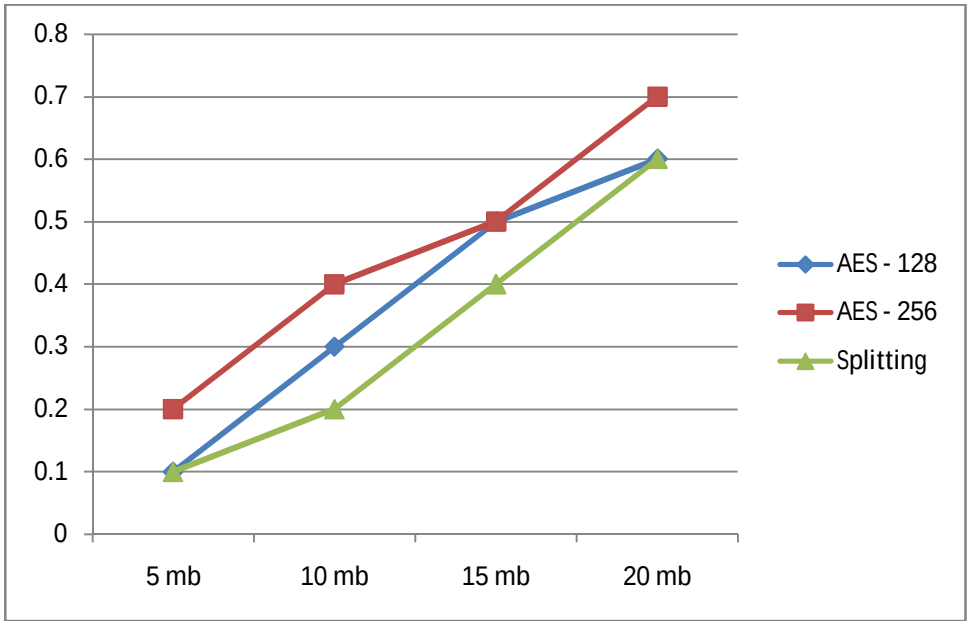
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018



The above graph shows the time taken by the different security algorithm to encrypt the different size data 5mb, 10mb, 15mb and 20mb. In this graph we have show the following security algorithms AES-128, AES-256 and our File Splitting Security algorithm and time taken by them to execute the data. With the help of graph it is clear that splitting takes less time and provides more security.

VIII. CONCLUSION

The Cloud Computing is the emerging technology and due to the increasing time it also gets expanding. According to the time, the users in the cloud are also increases and with this major challenge is the security of the information stored in the cloud server. In our work we have discussed the security algorithms like TDES, AES-128/256 with the comparison between them. Also we have introduced new security mechanism based on File Split. By go through all the results and graphs of the proposed work, we can conclude that our work is an efficient and effective secrecy based system increases performance of the cloud environment and also reduces the processing time. Also according the requirement of the information, they get that type of security. The framework shows that our proposed work provide the better security as compared to others.

As a part of the future work respective to our proposed work that this can be enhanced with better security algorithms like Asymmetric algorithm with better execution time, new techniques and methods used for providing better security to the information, other way data classification can also be used which enhance the system. Also soft computing techniques can be used which provide the automatic data classification and better techniques for the confidentiality and integrity of the information.

REFERENCES

[1]. Rizwana Shaikh, M. Sasikumar, “Security Issues in Cloud Computing: A Survey”, International Journal of Computer Applications, 2012.
[2]. Rizwana Shaikha , Dr. M. Sasikumar “Data Classification for achieving Security in cloud computing” Science Direct Procedia Computer Science 45 (2015) 493 – 498
[3]. Mr. Rupesh R Bobde , Amit Khaparde and Dr.M. M. Raghuwanshi “An Approach For Securing Data On Cloud Using Data Slicing And Cryptography”, IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015
[4]. Lo’ai Tawalbeh, Nour S. Darwazeh, Raad S. Al-Qassas, Fahd Aldosari, “A Secure Cloud Computing Model based on Data Classification”, Science Direct Procedia Computer Science 52 (2015) 1153 – 1158

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 10, October 2018

[5]. Gurpreet Singh, Supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013
[6] Ritu Tripathi, Sanjay Agrawal "Comparative Study of Symmetric and Asymmetric Cryptography Techniques" International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 1, Issue 6, June 2014. ISSN 2348 – 4853
[7]. Frank Simorjay, "Data Classification for Cloud Readiness", Microsoft Trustworthy Computing Doc. 2014.
[8]. Fara Yahya, Robert J Walters, Gary B Wills "Protecting Data in Personal Cloud Storage with Security Classifications", Science and Information Conference 2015 July 28-30, 2015 | London, UK
[9]. Nasrin Khanezaei, Zurina Mohd Hanapi " A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services", 2014 IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia
[10]. Dr. L. Arockiam, S. Monikandan, "Efficient Cloud Storage Confidentiality to Ensure Data Security", International Conference on Computer Communication and Informatics (ICCCI-2014).
[11]. Thanh Cuong Nguyen, Wenfeng Shen, Zhou Lei, Weimin Xu, Wencong Yuan, Chenwei Song, "A Probabilistic Integrity Checking Approach for Dynamic Data in Untrusted Cloud Storage", 978-1-4799-0174-6/13/$31.00 2013 IEEE.
[12]. CSA, "Top Threats to Cloud Computing V1.0, 2010.